OMB No. 0607-0725: Approval Expires: 08/31/2004

FORM **CS-1**
(7-26-2002)

2001 COMPUTER SECURITY SURVEY

U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU
Acting As Collecting Agent For
BUREAU OF JUSTICE STATISTICS
U.S. DEPARTMENT OF JUSTICE

DUE DATE:

RETURN COMPLETED FORM TO:

U.S. CENSUS BUREAU
1201 East 10th Street
Jeffersonville, IN 47132-0001

OR
FAX TO:
1–888–300–5192

For assistance, call
1–800–227–1735
Monday through Friday
8:00 a.m. to 5:00 p.m. EDT
OR
E-mail: css@census.gov

(Please correct any errors in name, address and ZIP Code)

NOTICE OF CONFIDENTIALITY – Your report to the Census Bureau is **confidential** by law (Title 13, Section 9 of the U.S. Code). It may be seen only by persons sworn to uphold the confidentiality of Census Bureau information and used only for statistical purposes from which no firm may be identified. The law also prohibits the sharing of your data with other agencies, exempts the information you provide from requests made under the Freedom of Information Act, and ensures that your responses are immune from legal process, including copies retained in your files.

Please refer to the enclosed instructions before completing the survey.

SURVEY SCOPE – This voluntary survey collects data on the type and frequency of computer security incidents in which a computer was used as the means of committing a crime against the company.

REPORTING ENTITY – Report consolidated figures for DOMESTIC OPERATIONS of this company, including all DIVISIONS, SUBSIDIARIES and LOCATIONS. If this company changed its operational status prior to or during the reporting period, see instructions.

REPORTING PERIOD – The reporting period for this survey is calendar year 2001. If 2001 calendar year figures are not available, please use fiscal year 2001 data.

ESTIMATES are acceptable.

I. COMPUTER SECURITY CONCERNS

1. What are the top three computer security concerns for this company? *Mark (X) three.*

101

01 ☐ Embezzlement
02 ☐ Fraud
03 ☐ Theft of proprietary information
04 ☐ Denial of service (to Internet connection or e-mail services)
05 ☐ Vandalism or sabotage (electronic)
06 ☐ Computer virus
07 ☐ Other intrusion or breach of computer system
08 ☐ Misuse of computers by employees (Internet, e-mail, etc.)
09 ☐ Unlicensed use or copying (piracy) of digital products – software, music, motion pictures, etc. – developed for resale
10 ☐ Other – *Specify*

II. COMPUTER INFRASTRUCTURE AND SECURITY

2a. In 2001, what types of computer networks did this company use? For this survey, "company" means DOMESTIC OPERATIONS, including all DIVISIONS, SUBSIDIARIES and LOCATIONS. *Mark (X) all that apply.*

201
- 01 ☐ Local area network (LAN)
- 02 ☐ Wide area network (WAN)
- 03 ☐ Process control network (PCN)
- 04 ☐ Virtual private network (VPN)
- 05 ☐ Electronic Data Interchange (EDI)
- 06 ☐ Wireless network (e.g., 802.11)
- 07 ☐ Internet
- 08 ☐ Intranet
- 09 ☐ Extranet
- 10 ☐ Stand-alone PCs (not on LAN)
- 11 ☐ Company has no computers – *(Skip to 20, page 8.)*
- 12 ☐ Don't know

b. In 2001, how many servers did this company have? 202 _____ Number

c. In 2001, how many individual PCs and workstations did this company have? 203 _____ Number

d. In 2001, which of the following types of access to its networks did this company support? *Mark (X) all that apply.*

204
- 01 ☐ Remote dial-in access
- 02 ☐ Access to networks through Internet
- 03 ☐ Wireless access to e-mail
- 04 ☐ Wireless access to Internet
- 05 ☐ Wireless access to this company's other networks
- 06 ☐ Publicly accessible website WITHOUT e-commerce capabilities
- 07 ☐ Publicly accessible website WITH e-commerce capabilities
- 08 ☐ Other – *Specify*
- 09 ☐ None of the above
- 10 ☐ Don't know

3a. In 2001, what types of computer system security technology did this company use? *Mark (X) all that apply.*

205
- 01 ☐ Anti-virus software
- 02 ☐ Biometrics
- 03 ☐ Digital certificates
- 04 ☐ E-mail logs/filters
- 05 ☐ System administrative logs
- 06 ☐ Encryption
- 07 ☐ Firewall
- 08 ☐ Intrusion detection system
- 09 ☐ One-time password generators (smartcards, tokens, keys)
- 10 ☐ Passwords (changed every 30 or 60 days, etc.)
- 11 ☐ Other – *Specify*
- 12 ☐ None; no computer security
- 13 ☐ Don't know

3b. In 2001, how much did this company spend on the types of computer system security technology identified in 3a? ESTIMATES are acceptable. EXCLUDE personnel costs.

	Mil.	Thou.	Dol.
206	$		

c. What percentage of this company's total 2001 Information Technology budget did this company spend on the types of computer system security technology identified in 3a? ESTIMATES are acceptable. *Round to nearest whole percent.* 207 _____ %

d. In 2001, was the amount this company spent on the types of computer system security technology identified in 3a more, less or about the same compared to the amount spent in 2000? *Mark (X) only one.*

208
- 01 ☐ More
- 02 ☐ Less
- 03 ☐ About the same/did not change
- 04 ☐ Don't know

e. In 2001, what computer security services did this company contract out to a third party? *Mark (X) all that apply.*

209
- 01 ☐ Evaluation of vulnerability
- 02 ☐ Intrusion/penetration testing of computer security
- 03 ☐ Installation of computer security
- 04 ☐ System administration of computer security
- 05 ☐ Other – *Specify*
- 06 ☐ None; all computer security was done in-house
- 07 ☐ Don't know

4a. In 2001, what types of computer security practices did this company have? *Mark (X) all that apply.*

210
- 01 ☐ Business continuity program for computer systems
- 02 ☐ Disaster recovery program for computer systems
- 03 ☐ Corporate policy on computer security
- 04 ☐ Regular review of system administrative logs
- 05 ☐ Periodic computer security audits
- 06 ☐ Formal computer security audit standards
- 07 ☐ Training employees in computer security practices
- 08 ☐ Other – *Specify*
- 09 ☐ None of the above
- 10 ☐ Don't know

b. If this company had a computer system business continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001? *Mark (X) all that apply.*

211
- 01 ☐ Tested
- 02 ☐ Used in emergency situation
- 03 ☐ Updated
- 04 ☐ None of the above
- 05 ☐ Don't know
- 06 ☐ Not applicable

III. TYPES OF COMPUTER SECURITY INCIDENTS

The questions in this section pertain to computer security incidents against this company, where the word "incident" refers to any unauthorized access, intrusion, breach, compromise or use of this company's computer system.

Computer security incidents may be committed by people either inside or outside the company and include embezzlement, fraud, theft of proprietary information, denial of service, vandalism, sabotage, computer virus, etc.

EXCLUDE incidents of unlicensed use or copying (piracy) of digital products – software, music, motion pictures, etc. – developed by this company for resale. These should be reported in Question 18.

Please do NOT duplicate information. If an incident can be classified under multiple categories, report it under the FIRST applicable category. For example, if proprietary information was stolen or copied by means of computer fraud, report it under fraud and do NOT include it under theft of proprietary information.

ESTIMATES are acceptable.

5. EMBEZZLEMENT

Embezzlement is the unlawful misappropriation of money or other things of value, BY THE PERSON TO WHOM IT WAS ENTRUSTED (typically an employee), for his/her own use or purpose.

INCLUDE instances in which a computer was used to wrongfully transfer, counterfeit, forge or gain access to money, property, financial documents, insurance policies, deeds, use of rental cars, various services, etc., by the person to whom it was entrusted.

a. Did this company detect any incidents in which a computer was used to commit embezzlement against this company in 2001?

301
01 ☐ Yes → **How many incidents were detected?** 302 _____ Number
02 ☐ No – *(If "No," skip to 6.)*

b. How many of these incidents were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center. 303 _____ Number

c. For the incidents in 5a, were any of the suspected offenders employed by this company at the time of the incident?

304
01 ☐ Yes → **In how many incidents?** 305 _____ Number
02 ☐ No
03 ☐ Don't know

d. What was the dollar value of money or other things taken by embezzlement in 2001? ESTIMATES are acceptable.

306

	Mil.	Thou.	Dol.
$			

e. What other monetary losses and costs were incurred in 2001 due to these incidents? ESTIMATES are acceptable. INCLUDE the cost of diagnosis, repair and replacement such as labor, hardware, software, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc. EXCLUDE costs associated solely with the prevention of future incidents.

307

	Mil.	Thou.	Dol.
$			

6. FRAUD

Fraud is the intentional misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM, or the use of electronic means to transmit deceptive information, in order to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.

INCLUDE instances in which a computer was used by someone inside or outside the company in order to defraud this company of money, property, financial documents, insurance policies, deeds, use of rental cars, various services, etc., by means of forgery, misrepresented identity, credit card or wire fraud, etc.

EXCLUDE incidents of embezzlement. Report these in 5.

a. Did this company detect any incidents in which someone inside or outside this company used a computer to commit fraud against this company in 2001?

308
01 ☐ Yes → **How many incidents were detected?** 309 _____ Number
02 ☐ No – *(If "No," skip to 7, page 4.)*

b. How many of these incidents were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center. 310 _____ Number

c. For the incidents in 6a, were any of the suspected offenders employed by this company at the time of the incident?

311
01 ☐ Yes → **In how many incidents?** 312 _____ Number
02 ☐ No
03 ☐ Don't know

d. What was the dollar value of money or other things taken by fraud in 2001? ESTIMATES are acceptable.

313

	Mil.	Thou.	Dol.
$			

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

6. FRAUD – Continued

e. What other monetary losses and costs were incurred in 2001 due to these incidents? ESTIMATES are acceptable. INCLUDE the cost of diagnosis, repair and replacement such as labor, hardware, software, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc. EXCLUDE costs associated solely with the prevention of future incidents.

314 $ | Mil. | Thou. | Dol.

7. THEFT OF PROPRIETARY INFORMATION

Theft of proprietary information is the illegal obtaining of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, personal or financial information, etc., usually by electronic copying.

EXCLUDE incidents which resulted in embezzlement or fraud. Report these in 5 or 6, page 3.

EXCLUDE incidents of unlicensed use or copying (piracy) of digital products – software, music, motion pictures, etc. – developed by this company for resale. Report these in 18, page 8.

a. Did this company detect any incidents in which someone inside or outside this company used a computer in order to obtain proprietary information from this company in 2001?

315
01 ☐ Yes → **How many incidents were detected?** 316 _____ Number
02 ☐ No – *(If "No," skip to 8.)*

b. How many of these incidents were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center.

317 _____ Number

c. For the incidents in 7a, were any of the suspected offenders employed by this company at the time of the incident?

318
01 ☐ Yes → **In how many incidents?** 319 _____ Number
02 ☐ No
03 ☐ Don't know

d. What was the dollar value of proprietary information taken by theft in 2001? ESTIMATES are acceptable.

320 $ | Mil. | Thou. | Dol.

e. What other monetary losses and costs were incurred in 2001 due to these incidents? ESTIMATES are acceptable. INCLUDE the cost of diagnosis, repair and replacement such as labor, hardware, software, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc. EXCLUDE costs associated solely with the prevention of future incidents.

321 $ | Mil. | Thou. | Dol.

8. DENIAL OF SERVICE

Denial of service is the disruption or degradation of an Internet connection or e-mail service that results in an interruption of the normal flow of information. Denial of service is usually caused by ping attacks, port scanning probes, excessive amounts of incoming data, etc.

INCLUDE incidents in which a virus, worm or Trojan horse was the cause of the denial of service.

a. Did this company detect any incidents of denial of service (a noticeable interruption of its Internet connection or e-mail service) in 2001?

322
01 ☐ Yes → **How many incidents were detected?** 323 _____ Number
02 ☐ No – *(If "No," skip to 9, page 5.)*

b. In 2001, how many of these incidents of denial of service were caused by a virus, worm or Trojan horse?

324 _____ Number

c. How many of these incidents in 8a were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center.

325 _____ Number

d. For the incidents in 8a, were any of the suspected offenders employed by this company at the time of the incident?

326
01 ☐ Yes → **In how many incidents?** 327 _____ Number
02 ☐ No
03 ☐ Don't know

e. What was the total duration (in hours) of the incidents of denial of service indicated in 8a? INCLUDE downtime needed for repairs.

328 _____ Hours

f. How many of these incidents of denial of service resulted in the company taking some action to restore the level of service?

329 _____ Number

g. How much was spent in 2001 to recover from these incidents of denial of service? ESTIMATES are acceptable. INCLUDE the cost – both internal and external – of diagnosis, repair and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future incidents.

330 $ | Mil. | Thou. | Dol.

h. What other monetary losses and costs were incurred in 2001 due to these incidents? ESTIMATES are acceptable. INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

331 $ | Mil. | Thou. | Dol.

i. How many of the incidents in 8a resulted in recovery costs or other monetary losses and costs reported above?

332 _____ Number

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

9. VANDALISM OR SABOTAGE (ELECTRONIC)

Vandalism or sabotage (electronic) is the deliberate or malicious damage, defacement, destruction, or other alteration of electronic files, data, web pages, programs, etc.

INCLUDE incidents of destructive viruses, worms, Trojan horses, etc.

EXCLUDE incidents of alteration which resulted in fraud. Report these in 6, page 3.

a. Did this company detect any incidents in which files, data, web pages or any part of its computer systems were electronically vandalized or sabotaged in 2001?

333
01 ☐ Yes → **How many incidents were detected?** 334 _____ Number
02 ☐ No – *(If "No," skip to 10.)*

b. How many of these incidents of vandalism or sabotage were caused by a destructive virus, worm or Trojan horse? 335 _____ Number

c. How many of these incidents in 9a were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center. 336 _____ Number

d. For the incidents in 9a, were any of the suspected offenders employed by this company at the time of the incident? EXCLUDE incidents in which an employee inadvertently executed a virus.

337
01 ☐ Yes → **In how many incidents?** 338 _____ Number
02 ☐ No
03 ☐ Don't know

e. How many of these incidents of vandalism or sabotage in 9a resulted in the downtime of this company's servers, routers, switches, individual PCs/workstations or websites? INCLUDE downtime needed for repairs. 339 _____ Number

f. What was the total downtime (in hours) of each of the following due to these acts of vandalism or sabotage? INCLUDE downtime needed for repairs.

1) Downtime of company websites/web servers 340 _____ Hours

2) Downtime of servers, routers or switches EXCLUDE downtime of websites/ web servers. 341 _____ Hours

3) Downtime of individual PCs/workstations EXCLUDE network-wide downtime reported above 342 _____ Hours

g. How much was spent in 2001 to recover from these incidents of vandalism or sabotage? ESTIMATES are acceptable. INCLUDE the cost – both internal and external – of diagnosis, repair and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future incidents.

343

	Mil.	Thou.	Dol.
$			

9. VANDALISM OR SABOTAGE (ELECTRONIC) – Continued

h. What other monetary losses and costs were incurred in 2001 due to these incidents? ESTIMATES are acceptable. INCLUDE actual losses such as the value of lost information. INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

344

	Mil.	Thou.	Dol.
$			

i. How many of the incidents in 9a resulted in recovery costs or other monetary losses and costs reported above? 345 _____ Number

10. COMPUTER VIRUS

A computer virus is a hidden fragment of computer code which propagates by inserting itself into or modifying other programs.

INCLUDE viruses, worms, Trojan horses, etc.

EXCLUDE incidents in which viruses caused excessive amounts of incoming data, resulting in denial of service. Report these in 8, page 4.

EXCLUDE incidents of destructive viruses, worms, Trojan horses, etc. Report these in 9.

a. In 2001, did this company intercept any computer viruses before they could infect any part of its computer systems?

346
01 ☐ Yes
02 ☐ No
03 ☐ Don't know
} – *(Continue with 10b.)*

b. Did this company detect any viruses which infected any part of its computer system in 2001? EXCLUDE viruses already reported in this survey.

347
01 ☐ Yes → **How many incidents of virus infections were detected?** *Count EACH DISTINCT INFECTION as a separate incident, even if caused by the same virus.* 348 _____ Number
02 ☐ No – *(If "No," skip to 11, page 6.)*

c. How many of these incidents were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center. 349 _____ Number

d. For the incidents in 10b, were any of the suspected offenders employed by this company at the time of the incident? EXCLUDE incidents in which an employee inadvertently executed a virus.

350
01 ☐ Yes → **In how many incidents?** 351 _____ Number
02 ☐ No
03 ☐ Don't know

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

10. COMPUTER VIRUS – Continued

e. What was the total number of infections for each of the following due to the computer virus incidents in 10b?

1) Number of server, router or switch infections 352 _____ Number

2) Number individual PC/workstation infections
INCLUDE infections resulting from server, router and switch infections AND infections from e-mail attachments, disks, internet downloads, etc. 353 _____ Number

f. What was the total downtime (in hours) for each of the following due to these virus infections?
INCLUDE downtime needed for repairs.

1) Downtime of servers, routers, or switches 354 _____ Hours

2) Downtime of individual PCs/workstations
EXCLUDE network-wide downtime reported above. 355 _____ Hours

g. How much was spent in 2001 to recover from these computer viruses? ESTIMATES are acceptable.
INCLUDE the cost – both internal and external – of diagnosis, repair and replacement such as labor, hardware, software, etc.
EXCLUDE costs associated solely with the prevention of future incidents.

356

	Mil.	Thou.	Dol.
$			

h. What other monetary losses and costs were incurred in 2001 due to these incidents? ESTIMATES are acceptable.
INCLUDE actual losses such as the value of lost information.
INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

357

	Mil.	Thou.	Dol.
$			

i. How many of the incidents in 10b resulted in recovery costs or other monetary losses and costs reported above? 358 _____ Number

11. OTHER COMPUTER SECURITY INCIDENTS

INCLUDE all other intrusions, breaches and compromises of this company's computer networks (such as hacking or sniffing) regardless of whether or not damage or loss were sustained as a result.

EXCLUDE incidents already reported in this survey.

a. Did this company detect any other computer security incidents in 2001?

359 360 _____ Number

01 ☐ Yes → **How many incidents were detected?**

02 ☐ No – *(If "No," skip to 12, page 7.)*

11. OTHER COMPUTER SECURITY INCIDENTS – Continued

b. Please briefly describe these computer security incidents.

361

c. How many of these incidents were reported to law enforcement, FedCIRC, ISAC or CERT? INCLUDE incidents reported to local, State or Federal law enforcement, the Federal Computer Incident Response Center, the Information Sharing and Analysis Center or the CERT® Coordination Center. 362 _____ Number

d. For the incidents in 11a, were any of the suspected offenders employed by this company at the time of the incident?

363

01 ☐ Yes → **In how many incidents?** 364 _____ Number

02 ☐ No

03 ☐ Don't know

e. How many of the other computer security incidents in 11a resulted in the downtime of this company's servers, routers, switches, individual PCs/workstations or websites? INCLUDE downtime needed for repairs. 365 _____ Number

f. If any, what was the total downtime (in hours) of each of the following due to these other computer security incidents?
INCLUDE downtime needed for repairs.

1) Downtime of company websites/web servers 366 _____ Hours

2) Downtime of servers, routers or switches
EXCLUDE downtime of websites/ web servers. 367 _____ Hours

3) Downtime of individual PCs/workstations
EXCLUDE network-wide downtime reported above 368 _____ Hours

g. How much was spent in 2001 to recover from these computer security incidents? ESTIMATES are acceptable.
INCLUDE the cost – both internal and external – of diagnosis, repair and replacement such as labor, hardware, software, etc.
EXCLUDE costs associated solely with the prevention of future incidents.

369

	Mil.	Thou.	Dol.
$			

h. What other monetary losses and costs were incurred in 2001 due to these incidents? ESTIMATES are acceptable.
INCLUDE actual losses such as the value of lost information.
INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

370

	Mil.	Thou.	Dol.
$			

i. How many of these incidents in 11a resulted in recovery costs or other monetary losses and costs reported above? 371 _____ Number

IV. SPECIFIC INCIDENT INFORMATION

For Questions 12–15, please report for the single most significant computer security incident for this company in 2001. If there were multiple similar incidents, choose ONE representative incident.

12. For the incidents reported in this survey, in what month did this company's single most significant computer security incident occur? 401 _____ Month

13a. Which of this company's computer networks were affected in this particular incident? *Mark (X) all that apply.*

402

- 01 ☐ Local area network (LAN)
- 02 ☐ Wide area network (WAN)
- 03 ☐ Process control network (PCN)
- 04 ☐ Virtual private network (VPN)
- 05 ☐ Electronic Data Interchange (EDI)
- 06 ☐ Wireless network (e.g., 802.11)
- 07 ☐ E-mail system
- 08 ☐ Internet
- 09 ☐ Intranet
- 10 ☐ Extranet
- 11 ☐ Individual workstation (on LAN)
- 12 ☐ Stand-alone PC (not on LAN)
- 13 ☐ Other – *Specify*
- 14 ☐ Don't know
- 15 ☐ Not applicable

b. Which of the following were used to access this company's networks in this particular incident? *Mark (X) all that apply.*

403

- 01 ☐ Hard-wired communications lines
- 02 ☐ Remote dial-in access
- 03 ☐ Access to networks through Internet
- 04 ☐ Wireless access to e-mail
- 05 ☐ Wireless access to Internet
- 06 ☐ Wireless access to this company's other networks
- 07 ☐ Publicly accessible website WITHOUT e-commerce capabilities
- 08 ☐ Publicly accessible website WITH e-commerce capabilities
- 09 ☐ Other – *Specify*
- 10 ☐ None of the above
- 11 ☐ Don't know
- 12 ☐ Not applicable

c. If this particular incident resulted in any downtime, what was the total duration (in hours) of each of the following? INCLUDE downtime needed for repairs.

1) Denial of service (to Internet connection or e-mail services) 404 _____ Hours

2) Downtime of company websites/ web servers 405 _____ Hours

3) Downtime of servers, routers or switches EXCLUDE downtime of websites/ web servers. 406 _____ Hours

4) Downtime of individual PCs workstations EXCLUDE network-wide downtime reported above. 407 _____ Hours

d. How much was spent in 2001 to recover from this particular incident? ESTIMATES are acceptable. INCLUDE the cost – both internal and external – of diagnosis, repair and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
408 $			

e. In this particular incident, what was the dollar value of money or other things taken or lost (by embezzlement, fraud, theft, vandalism, sabotage, etc.)? ESTIMATES are acceptable.

	Mil.	Thou.	Dol.
409 $			

13f. What other monetary losses and costs were incurred in 2001 due to this incident? ESTIMATES are acceptable. INCLUDE the estimate value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

	Mil.	Thou.	Dol.
410 $			

g. Which of the following types describes this particular incident? *Mark (X) only one.*

411

- 01 ☐ Embezzlement
- 02 ☐ Fraud
- 03 ☐ Theft of proprietary information
- 04 ☐ Denial of service (to Internet connection or e-mail service
- 05 ☐ Vandalism or sabotage (electronic)
- 06 ☐ Computer virus
- 07 ☐ Other computer security incident – *Specify*
- 08 ☐ Not applicable

14a. To which of the following organizations was this incident reported? *Mark (X) all that apply.*

412

- 01 ☐ Local law enforcement
- 02 ☐ State law enforcement
- 03 ☐ FBI (Federal Bureau of Investigation)
- 04 ☐ FedCIRC (Federal Computer Incident Response Center)
- 05 ☐ Other government agency – *Specify*
- 06 ☐ ISAC (Information Sharing and Analysis Center)
- 07 ☐ CERT® Coordination Center
- 08 ☐ None of the above

b. If this incident was not reported to any of the organizations listed in 14a, what were the reasons? *Mark (X) all that apply.*

413

- 01 ☐ Negative publicity
- 02 ☐ Lower customer/client/investor confidence
- 03 ☐ Competitor advantage
- 04 ☐ Incident outside jurisdiction of law enforcement
- 05 ☐ Reported elsewhere – *Specify*
- 06 ☐ Did not want data/hardware seized as evidence
- 07 ☐ Did not know who to contact
- 08 ☐ Did not think to report
- 09 ☐ Nothing to be gained/nothing worth pursuing
- 10 ☐ Other – *Specify*

15. What was the relationship between the suspected offender and this company at the time of this particular incident? *Mark (X) only one.*

If there were multiple offenders, answer for the one viewed as the principal offender.

414

- 01 ☐ Current employee, contractor, temporary worker, etc.
- 02 ☐ Former employee, contractor, temporary worker, etc.
- 03 ☐ Domestic competitor
- 04 ☐ Foreign competitor – *Specify country*
- 05 ☐ Foreign hacker – *Specify country*
- 06 ☐ Hacker (no known association with this company)
- 07 ☐ Other – *Specify*
- 08 ☐ Don't know

V. OTHER TRENDS IN COMPUTER SECURITY

16. In 2001, was the overall number of computer security incidents detected by this company more, less or about the same compared to the number detected in 2000? *Mark (X) only one.*

501
01 ☐ More
02 ☐ Less
03 ☐ About the same/did not change
04 ☐ Don't know

17. In 2001, did this company have a separate insurance policy or rider to cover losses due specifically to computer security breaches?

502
01 ☐ Yes
02 ☐ No
03 ☐ Don't know

18a. In 2001, which of the following types of digital products did this company develop for resale? *Mark (X) all that apply.*

503
01 ☐ Software
02 ☐ Music
03 ☐ Motion pictures
04 ☐ Other – *Specify* _____
05 ☐ None; company did not produce digital products for resale in 2001 – *(If "None," skip to 19a.)*

b. In 2001, did this company experience any unlicensed use or copying (piracy) or digital products which it developed for resale?

504
01 ☐ Yes
02 ☐ No
03 ☐ Don't know } *(Skip to 19a.)*

c. What was the estimated revenue lost in 2001 due to this unlicensed use or copying?

	Mil.	Thou.	Dol.
505 $			

VI. COMPANY INFORMATION

19a. In 2001, which of the following Internet services, if any, did this company provide? *Mark (X) all that apply.*

601
01 ☐ Internet Service Provider (ISP)
02 ☐ Web Search Portal
03 ☐ Internet Publishing
04 ☐ Internet Broadcasting
05 ☐ None of the above – *(Skip to 20.)*

b. In 2001, which of the following Internet services, if any, was the PRIMARY business activity for this company? *Mark (X) only one.*

602
01 ☐ Internet Service Provider (ISP)
02 ☐ Web Search Portal
03 ☐ Internet Publishing
04 ☐ Internet Broadcasting
05 ☐ None of the above

VI. COMPANY INFORMATION – Continued

20. What were the total sales, receipts, and operating revenue for this company in 2001? ESTIMATES are acceptable.

	Bil.	Mil.	Thou.	Dol.
603 $				

21. What was the total number of employees on this company's payroll for the pay period which includes March 12, 2001? Estimates are acceptable. *Count EACH part-time employee as one. EXCLUDE contractors, leased and temporary employees.*

604 _____ Number

22. Does the information reported in this survey cover the calendar year 2001?

605
01 ☐ Yes
02 ☐ No – *Specify period covered:*

	Month	Year
FROM 606	/	
TO 607	/	

23. What was this company's operational status at the end of 2001? *Mark (X) only one.*

608
01 ☐ In operation
02 ☐ Under construction, development, or exploration
03 ☐ Temporary or seasonally inactive
04 ☐ Ceased operation
05 ☐ Sold or leased to another operator } → 609 Month / Year /

Successor company:

Company Name

Street address

City | State | Zip code

CONTACT INFORMATION

Person to contact regarding this report:

Name

Title

Telephone number ( ) | Extension

Fax number ( )

E-mail address

Use a separate sheet of paper for any explanations that may be essential in understanding your reported data. Please make a copy for your records.